Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

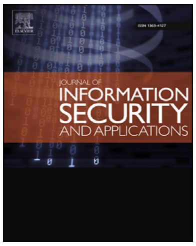

Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB

H. Dadgostar [a], F. Afsari [b,*]

[a] *Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran*
[b] *Department of Computer Engineering, Shahid Bahonar University of Kerman, Kerman, Iran*

ARTICLE INFO

Article history:
Available online

Keywords:
Steganography
Modified LSB
Interval-valued intuitionistic fuzzy sets
Edge detection

ABSTRACT

The Internet is becoming increasingly popular as a communication channel. However, message transmissions via the Internet have some problems, such as information security, copyright protection, and so on. Therefore, we need a secure communication method to transmit messages via the Internet. Steganography is a technique that hides secret data into cover media by altering its most insignificant components, such that an unauthorized user will not be aware of the existence of the secret data. In recent years the development of artificial intelligence and fuzzy logic has started a new period in the whole science. The proposed scheme has taken into consideration the property that more information can be hidden into the edge areas rather than in the smooth areas. This scheme makes the use of interval-valued intuitionistic fuzzy edge detecting method as well as the modified LSB substitution method that causes the image quality and capacity to increase. The use of intuitionistic fuzzy sets not only improves the image quality, but it is also more accurate in detecting the edges and smooth areas. The proposed scheme is tested on different standard images with secret messages of various lengths. The experimental results show the ability of the proposed scheme.

1. Introduction

The use of the Internet is increasing day by day and transferring important information through it is also increasing. The security of important information is necessary during transferring it via the Internet. Therefore, a secure communication method is necessary. Encrypting such information is one of the ways to provide security. In the encryption method, information is changed in such a way that intruders cannot read the information. But during encryption, the message is changed, therefore it is distorted and an intruder may easily suspect the presence of confidential information. Steganography is another way of securing secret information. The word steganography is obtained from the Greek words "stegos", meaning "cover", and "grafia", meaning "writing", defining it as "covered writing". Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion (Provos and Honeyman, 2003). Steganography is separated from cryptography in the aspect that one of steganography's basic aims is that the secret data is hidden but nobody should understand that there are data embedded, while in cryptography everybody knows that there is a secret message (Wu and Tsai, 2003). Image steganography, where secret data is embedded within an image, as a cover media, has been widely

[*] *Corresponding author.* Shahid Bahonar University of Kerman, PO Box: 76169-133, Pajouhesh Square, Kerman, Iran. Fax: +98 34 33257501.
E-mail address: afsari@uk.ac.ir, afsari.f@gmail.com (F. Afsari).

http://dx.doi.org/10.1016/j.jisa.2016.07.001

Please cite this article in press as: H. Dadgostar, F. Afsari, Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB, Journal of Information Security and Applications (2016), doi: 10.1016/j.jisa.2016.07.001

studied during the last decades. Content adaptability, visual resilience, smaller size of images and also the weaknesses of the human visual system (HVS) (Kanan and Nazeri, 2014) make it a good carrier to transmit secret messages over the Internet. Image steganography can be broadly classified into spatial domain, transformation domain, spread spectrum and model based steganography. In spatial domain, secret message is embedded in pixel value directly whereas transformation domain methods achieve embedding by first transforming the image from spatial to frequency domain using any one of the transforms such as discrete cosine transform (DCT), discrete wavelet transform (DWT), Hadamard transform, Dual tree DWT, double density dual tree DWT (DD DT DWT), ridgelet transform, curvelet transform, and so on. Then embedding is done in suitable transform coefficients. Various techniques can be employed to optimally choose the transform coefficients to hide data in. Soft computing tools can be considered for this purpose. As transformation domain methods are more immune to image processing operations and are less susceptible to stego attacks, they are usually preferred over spatial domain methods. Spread spectrum steganography involves embedding in noise which is inherent from the image acquisition process. Image restoration and error control techniques can be used while extracting the data at the decoder side. It is a blind scheme as the original image is not required during extraction. This scheme outperforms others in terms of payload capacity and invisibility. Model based steganography is based on the statistical model of the cover image. It is also known as statistics aware embedding. Before selecting the locations for data hiding in a cover image, statistical global features of the image are taken into account and then the actual data embedding process is carried out accordingly. Thus, it provides an additional layer of security to steganography (Subhedar and Mankar, 2014). Also, there are two main approaches to achieve embedding in spatial domain that are categorized as Least-Significant-Bits (LSB) substitution, and Pixel-Value-Differencing (PVD). LSB substitution is the most commonly used method directly replacing the LSBs of pixels in the cover image with secret bits to get the stego image (Chang et al., 2002). PVD method provides good imperceptibility by calculating the difference of two consecutive pixels to determine the depth of the embedded bits (Liu and Shih, 2008).

The proposed scheme is a kind of spatial domain technique where the secret message is embedded in the LSBs. In this paper, *Cover image* refers to the image used for carrying the embedded bits, the embedded data is known as *payload* and the image with the embedded data is called as *stego image*. Some of the major requirements of steganography include capacity, robustness and security. *Robustness* indicates the amount of modification that the stego image can withstand before an adversary can destroy hidden information. *Capacity* refers to the amount of information that can be hidden in cover image without deteriorating the integrity of the cover image. It is represented in terms of bits per pixel (bpp). Embedding operation needs to preserve the statistical properties of the cover image in addition to the perceptual quality. *Security* means eavesdropper's inability to detect hidden information (Subhedar and Mankar, 2014). Security of any steganography technique depends on the selection of pixels for embedding. Pixels in noisy and textured areas are better choices for embedding because they are difficult to model. Pixels in edges can be seen as noisy pixels because their intensities are either higher or lower than their neighboring pixels due to sudden change in the coefficient gradient. Due to these sharp changes in the visual and statistical properties, edges are difficult to model in comparison to pixels of smoother area. Thus a potential edge detecting method is needed. In this paper, interval-valued intuitionistic fuzzy edge detector algorithm (Afsari et al., 2014) has been applied to distinguish between edge and non-edge pixels. Also, the edge detection method should give the same results after embedding. To this end, in the proposed scheme, just the MSBs of each pixel concern in the edge detection algorithm and the secret data is embedded in the remaining LSBs. Thus the edges before and after embedding will not change. It is worth noting, in the proposed scheme, the amount of information which is hided in edge areas using LSB technique is more compared to smooth areas. Also, a modified LSB substitution technique has been used to have better imperceptibility. Finally, using the combination of edge detection algorithm and modified LSB substitution technique, the capacity of hidden data and imperceptibility of image can be increased. Performance of the proposed technique is analyzed on a large image database containing 500 gray scale images.

The rest of the paper is organized as follows. Several steganography techniques have been reviewed in Section 2. The proposed efficient adaptive edge based steganography scheme has been proposed in Section 3. Section 4 demonstrates the experiment setup, results and analysis. Finally, Section 6 concludes the paper.

2. Literature review

Generally, LSB techniques replace the same length bits of each original pixel with the embedding data. However, not all pixels in the image can tolerate equal amounts of changes without noticeable distortion (Yang et al., 2008). Therefore, the stego image has low quality when equally changing LSBs of all pixels. To solve this issue, some LSB based methods employed HVS masking characteristics to embed the secret data into the variable sizes of LSBs of each pixel. Lie and Chang (1999) created a piecewise mapping function according to the HVS contrast sensitivity to determine the adaptive numbers of LSBs for data hiding. Lee and Chen (2000) exploited the contrast and luminance property of HVS and achieved a variable-sized LSB insertion. In Liu et al.'s methods (2004), each pixel of the original image is grouped according to its intensity, then the frequency of the original pixel in each group is counted, and a bit plane wise data hiding method is used to embed the secret message into the original image by the principle of the pixel with high frequency priority. Similarly, Kekre et al. (2008) determined the embedded capacity of each pixel by considering the luminance from the highest bits residual image. Wang (2015) tries to adopt the famous Median edge detection (Med) to distinguish between the flat area and the complex area. This research applies Least Significant Bit and the optimal pixel adjustment process method to embed the confidential information for reducing the distortion. To further improve the quality of the stego image, some PVD methods (Wang et al., 2008; Wu

Please cite this article in press as: H. Dadgostar, F. Afsari, Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB, Journal of Information Security and Applications (2016), doi: 10.1016/j.jisa.2016.07.001